



Oppose So-Called “Right to Repair” Bill (H.R. 906)

Legislation Raises Serious Vehicle Privacy, Security and Safety Issues for Consumers

ISSUE

Advocates for “right to repair” legislation claim that independent automotive repair shops do not have access to the parts or data necessary to repair vehicles. However, this concern was rectified by a 2014 Memorandum of Understanding, signed by “right to repair” proponents and auto manufacturers, and reaffirmed by a [2023 industry commitment](#). Today, the information independent shops need to repair vehicles is readily [available](#) from every auto and truck manufacturer. [H.R. 906](#) has little to do with repairing a vehicle; instead, the bill compels auto and heavy-duty truck manufacturers to provide any “aftermarket parts manufacturer” the information necessary “to produce or offer compatible aftermarket parts,” i.e., parts not made by the auto or truck manufacturer. This legislation would also give any third-party remote, bidirectional access to consumer data from vehicles, which raises significant privacy, cybersecurity, and automotive safety concerns. This bill regulates only vehicles and does not apply to other products, such as farm equipment or mobile phones. **Members of Congress should oppose H.R. 906 since it has little to do with repairing a vehicle while raising serious vehicle privacy, security and safety issues for consumers.**

BACKGROUND

H.R. 906 would require vehicle manufacturers to provide any third-party remote, bidirectional access to vehicle-generated data “without restrictions or limitations.” This overbroad requirement which covers *all* the vehicle’s data, including data unrelated to the servicing of the vehicle, creates serious privacy and safety concerns. Automakers and independent repairers already have a longstanding formal mechanism through the [National Automotive Service Task Force](#) to ensure service information, tool information and training data is made available from every truck and auto manufacturer. This information is also available through several private companies.

The National Highway Traffic Safety Administration [has noted](#) the “significant safety concerns” open access to vehicle telematics would raise, stating, “Open access to vehicle manufacturers’ telematics offerings with the ability to remotely send commands allows for manipulation of systems on a vehicle, including safety-critical functions such as steering, acceleration, or braking... A malicious actor here or abroad could utilize such open access to remotely command vehicles to operate dangerously, including attacking multiple vehicles concurrently.” NADA re-emphasized NHTSA’s vehicle safety concerns in a [letter](#) to the House Energy and Commerce Committee.

In this vein, the Department of Commerce issued [an advance notice of proposed rulemaking](#) to consider potential vehicle technology vulnerabilities and to address national security risks posed by connected vehicles, specifically Chinese-manufactured technology.

KEY POINTS

- **This legislation undermines intellectual property rights.** H.R. 906 unfairly promotes the interests of aftermarket companies by compelling auto and truck manufacturers to provide any “aftermarkets parts manufacturer” the information necessary “to produce or offer compatible aftermarket parts.” This giveaway of proprietary information would allow aftermarket parts manufacturers to gain access to automakers’ proprietary information which could then be used to facilitate the reverse engineering of genuine, original auto and trucks parts, including safety-critical parts.
- **A recent Government Accountability Office (GAO) report confirms the information and tools necessary to repair vehicles are already available to independent repair shops.** The report found that of the eight automakers GAO interviewed, all confirmed that “they provide to independent repair shops, on fair and reasonable conditions, equal access to the information, data, and tools needed for repairs, and will continue to do so.” Independent repair shops currently perform more than 70% of all non-warranty repairs, and according to the Auto Care Association, their total revenue grew 43% from 2014-2022.
- **H.R. 906 creates new privacy, vehicle security and safety risks.** The bill would force manufacturers to release information that could create serious privacy, data security and vehicle safety risks. For example, the bill mandates that vehicle manufacturers provide *all* “vehicle-generated” data unconditionally, which may include sensitive private information, to any person the vehicle owner has designated.

STATUS

Despite numerous concerns articulated on a bipartisan basis by members of the House Subcommittee on Innovation, Data and Commerce, that subcommittee reported out H.R. 906 on Nov. 2. NADA and other industry stakeholders submitted a [coalition letter](#) opposing this fundamentally flawed legislation. **Members of Congress are urged not to cosponsor H.R. 906.**